Tim Yardley
University of Illinois
J. Ritchie Carroll
Grid Protection Alliance

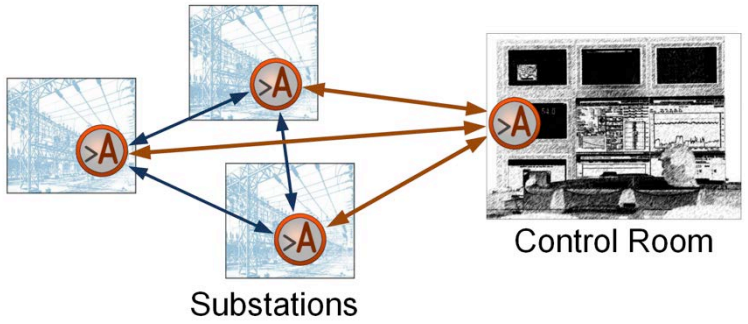
ARMORE: Applied Resiliency for More Trustworthy Grid Operation

Cybersecurity for Energy Delivery Systems Peer Review
August 5-6, 2014

ARMORE: Summary

- **Objective**

  To develop a distributed peer-based framework to provide secure information exchange internally in critical infrastructure to increase security and resiliency of grid operation through seamless enhancement of legacy and modern protocols.



- **Schedule**

  October 2013 – September 2016

  - Final design - 9/15/14
  - Alpha Version - 9/15/15
  - Demonstration - 6/15/16
  - Version 1.0 released - 9/15/16

- **Total Value of Award:** $2.85M (15% funds expended to date)
- **Performers:** Grid Protection Alliance, University of Illinois
- **Testing Partner:** PNNL

ARMORE: Technical Approach and Feasibility

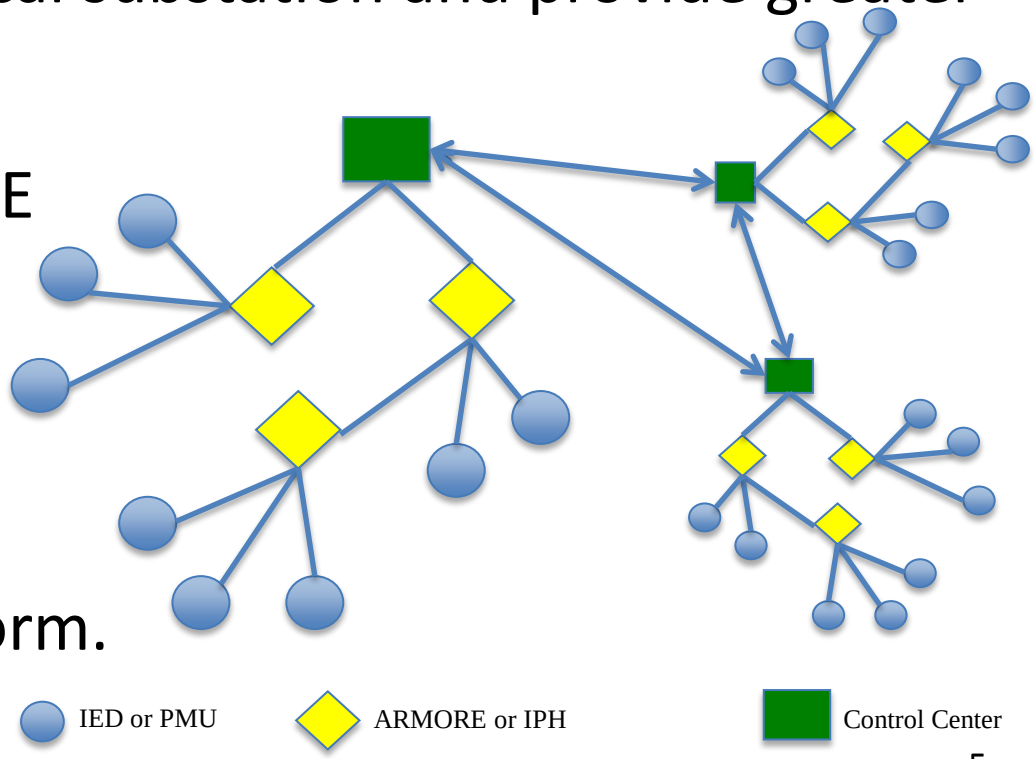
- **Current Situation**
  - Centralized data aggregation and perimeter-level security
  - Need for protection from within the security perimeter
- **Development Approach**
  - **Security Enhancement**
    - Encapsulation
    - Inspection and Policy Enforcement
  - **Progressive Enhancement**
    - Security features for all protocols
    - Even more enhancement for known protocols
  - **Interoperable Deployment**
    - Transparent operation
    - Middleware layer for easy integration
  - **Free, Open Source**
    - Accelerated innovation
    - Integrating with a well-proven codebase

ARMORE: Technical Approach and Feasibility

- ARMORE will pave the way toward more real-time data-driven and secure control of the grid as a whole.
- ARMORE leverages a defense-in-depth approach that advances the security footprint of a utility and extends the envelope of protection from the external perimeter to the inside of the utility.
- ARMORE will be built using lessons-learned from many projects before it, including CONES, SIEGate, OPSAID, LEMNOS and others.

ARMORE: Technical Approach and Feasibility

- ARMORE will be designed to support a high-speed peer-based communications while honoring current regulatory requirements for establishment of Electronic Security Perimeters for each critical substation and provide greater overall security.
- Where possible, ARMORE will leverage core components of the successful Secure Information Exchange Gateway (SIEGate) platform.

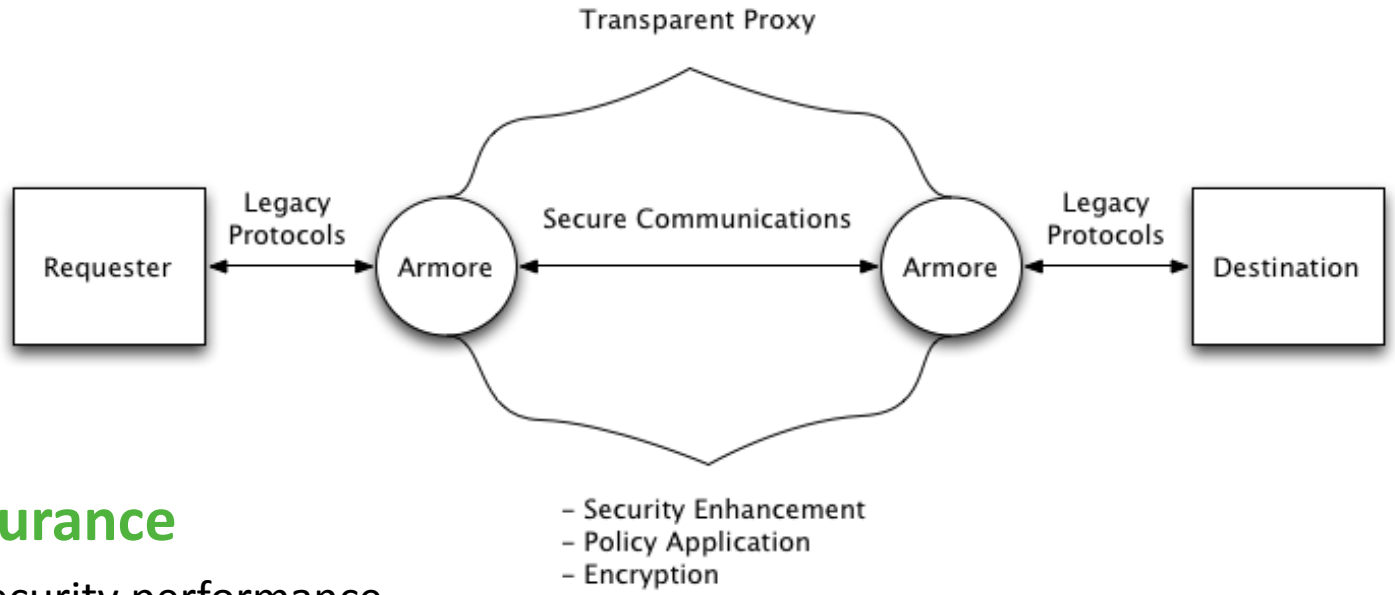


ARMORE: Technical Approach and Feasibility

- **Challenges to Success**
  - Accurate and complete identification of all functional, security, and performance requirements for common intra-organizational operations in the utility industry
    - *Overcome by use of project team expertise to ensure use cases cover a wide range of operating requirements and incorporation of best practice security methodologies*
  - Ability to reliably provide inline security in a transparent way that is both interoperable and resilient
    - *Overcome by modular architecture and implementation of a middleware communication layer while building on tested technologies like SIEGate and Bro IDS.*

ARMORE: Technical Design Challenges

- **Performance given system complexity**
  - Transparently proxy data of both known and unknown types
  - Support multiple data types efficiently and securely
  - Minimize latency and maximize throughput

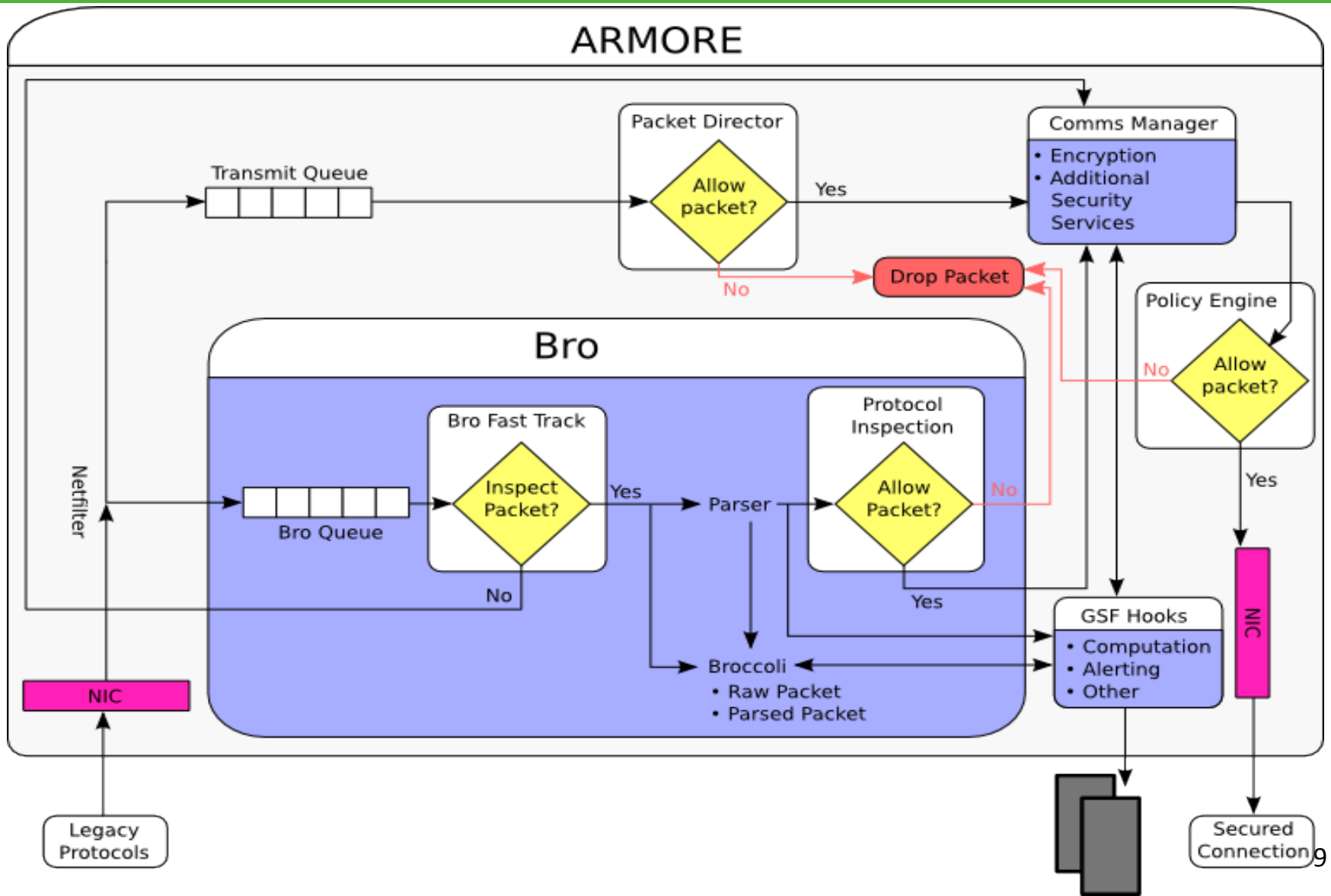


- **Security assurance**
  - Maximize security performance
  - Minimize security breach impact

ARMORE: Technical Design Principles

- Provide extensibility through component based architecture
- Leverage the concept of progressive enhancement
- Build on the successes of tested technologies
- Design with both resilience and reliability from the ground-up with security integrated from the beginning
- Provide flexibility to be active or passive for enforcement of security policies, but always provide enhanced communication

ARMORE: Conceptual Data Flow Diagram



ARMORE: Development Progress

- **Technical Achievements to Date**
  - Met with industry contacts to evaluate use cases and validate design approach
  - Research into design options
  - Draft of design document completed
  - Implementation feasibility being explored on various components of the system

Collaboration/Technology Transfer

- ARMORE technology transfer activities will be targeted at prospective vendors (equipment developers and producers) and users (electric utility industry)
- The project team will ensure ongoing involvement of vendors and users by early dissemination of open source alpha and beta versions and incorporating identified issues into hardware and software revisions
- Demonstration systems will be deployed and tested in real-world sites and situations

Next Steps for this Project

- Issue final design document – 9/15/14
- Release Alpha Version of ARMORE – 9/15/15
- Complete ARMORE bench test – 12/15/15
- Deploy ARMORE for demonstration - 6/15/16
- Release Open Source Version 1.0 – 9/15/16

- **Links to other projects**
  - Research is ongoing into using the Bro Network Security Monitor project as a base technology for ARMORE

Applied Resiliency for More Trustworthy Grid Operation

Questions?

GRID PROTECTION ALLIANCE

1867 ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability